European Aviation Safety Agency

RTCA SC-214/EUROCAE WG-78

Air Traffic Services Safety and Interoperability Requirements

General Information

Paper Reference: **POS-PL-EASA Issues**	Revision: -	Date: Oct 2012	Status :
Editor / Author: EASA Avionics (Point of Contact: A. D. Mancebo)	Review Meeting/Teleconference: October 22 - 26, 2012 Comments Due:		

Position Paper Title:

Issues with Safety assessment (OSA) for CPDLC

Abstract and Proposed Action:

This position paper identifies issues, impacts, and recommendations for SC-214/WG-78 to be reviewed and commented during its next Sub-Group session. Resolution and agreement of these issues is critical in order to consider the SPR as an acceptable means of compliance:
- for the future approval of CPDLC beyond the actual use (cruise flight phase over upper airspace), and
- the consideration of this standard within the European SESAR packages, without any further need of additional requirements to be developed by EASA.

EASA invites SC-214/WG-78 to collaborate on determining mutually acceptable resolutions to the issues at the earliest possibility.

Issues relating to safety assessment and human error rate are to be considered as the highest priority.

Key words (Optional):

EASA Issues, Safety Assessment, OSA

Distribution

SC-214/WG-78Groups	***Additional Names***	***Additional Names***	***Additional Names***
Plenary			
CSG			
VSG			

1 Introduction

1.1 Existing SPR standards (already published by RTCA and EUROCAE) are currently providing safety and performance requirements for implementations of ATS communications, during cruise flight phase, within European continental upper airspace (ED120/DO290) and oceanic and remote airspace throughout the Asia-Pacific Region, North Atlantic Region, and the South Atlantic Sub-Region (ED-122/DO-306). The SC-214/WG-78 SPR standard is intended to provide safety and performance requirements for next generation implementations of ATS data communications for all types of airspace (i.e., Domestic, Oceanic/Remote, and for a converged aircraft equipage package).

1.2 The current draft of the Terms of Reference (TORs) calls for data communication standards to support NextGen and SESAR initiatives that can be applied to domestic, oceanic and remote airspace uniformly worldwide. The primary need for the SPR standard publication is for regulatory promulgation to serve as the basis for means of compliance for type design approvals, operational authorizations and safety oversight of air traffic service provisions.

1.3 The European Aviation Safety Agency (EASA) has reviewed the current draft OSA (Rev H) and identified a number of issues requiring attention. EASA aims to avoid any exceptions in recognizing SC-214/WG-78 products as regulatory means of compliance. EASA also wants to avoid to develop additional requirements to guarantee that the required safety levels are achieved within the scope of SESAR programs.

1.4 This paper provides in Section 2 a description of each issue categorized as follows:

2.1.- Human error rate concept

2.2.- Non-coherent definition of SW development assurance levels

2.3.- Issues within the assessment

2.3.1. Issue with regards to independence

2.3.2. Common modes

2.3.3. Worst cases and identification of the precise intended use of the functions supported by CPDLC

2.3.4. HW failures

2.3.5. No safety objective for DLIC service

2.3.6. Issue with regards to classification of hazards

2.3.7. Unit conversion

2.3.8. Questionable assumptions

2.3.9. Removal of human error contribution from all fault tree analyses

2.3.10. Issue with regards to the terminology used in the OSA

2.3.11. Additional comments

1.5 SC-214/WG-78 is invited to agree on the priority of the issues and collaborate on determining mutually acceptable solutions to resolve the issues.

2.1. Human Error Rate concept

The use of Human Error Rates as proposed in this OSA is strongly rejected by EASA.

Even if it seems that the technique can allow for the direct quantification of human error probability (HEP), and also that could be easily integrated into typical methods for safety analysis, EASA rejects it because it requires to make several assumptions and compromises that limit the level of confidence that we can have in the probabilities that are generated.

- The probabilities that CARA uses are derived from the Generic Task Types (GTT) and Error Producing Conditions (EPC) that were originally created for use in non-aviation domains. The authors used expert opinion and educated guesses to correlate these non-ATM GTT's and EPC's onto ATM specific tasks.
- The human error rate in itself is not the major item which needs to be evaluated. It is more important to determine how human error could occur, the possibilities of its detection and its contribution to a given operational hazard with its associated operational procedure. This is why the involvement of air traffic controllers, pilots, and operations experts seems essential for the estimation of the human performance.
- CARA requires some kind of task analysis; i.e., decomposition of events into sub-tasks. The confidence that one can have in the output from CARA depends heavily upon the quality of this analysis. Unfortunately, there is not a universal standard in human factors that defines the "best level" of decomposition. This means that CARA analysis performed by different people could produce different probabilities.
- It cannot account for novel failure modes arising from new operations.
- EASA AMC to CS-25.1309 section 12 clearly states that "quantitative assessments of crew errors are not considered as feasible". For this reason, AMC to CS-25.1309 allows taking credit of crew or maintenance actions for reasonable tasks to be defined respectively in the AFM or the AMM. EASA's position is in line with FAA's position who issued in November 2010 a position paper stating the following: "Quantification of likelihood estimates for human error, especially for those events without a documented history, may result in inaccurate, unreliable and severely misleading probability estimates."(ref. POS-PL-FAA Issues, 5.2.4.b).

Additionally, the CARA approach that is described may be criticized because:

- It is not understood how a reliable value can be provided. It seems to imply that, at the end, an expert judgment is still needed to determine an "objective" probability, which is unacceptable.
- The likelihood of an error is not the only parameter to consider. Actually a lot of parameters have to be taken into account: is an error easily detectable? Is it recoverable? What are the safety consequences? Can those consequences be mitigated by other pieces of the Human/Machine system? As an example, some errors that occur very often may not be necessarily mitigated by redesign or other means when the safety consequences are definitely not critical, whereas a single occurrence of one critical error, observed in a representative environment, may lead to significant actions.
- This is generally associated with a systematic approach. The issue is that prior analyzing the probability of a human error, one will have to identify all the potential human errors, which is totally unrealistic. The adverse effect is that this can lead to missing a lot of potentially critical human errors.
- A detailed task analysis does not fit with a performance-based approach for the procedures in the cockpit. Not all cockpits are similar. The integration of an operational procedure into a cockpit also has to fit the airline operations and training. A task analysis would only be relevant for a given airline and aircraft type. On the other hand, the SPR should only define the generic principles of the operational procedure.

Moreover, in the frame of the airborne certification exercise (CS 25.1302, human factors assessment), EASA does not require quantification of human errors. The approach is based on the opportunistic observation of errors during the demonstration process. There is a significant amount of human factors evaluations during this process from which one can be confident that the largest part of the occurrences that can be "reasonably expected in service" for a particular type have been spotted, analysed and mitigated if applicable. Obviously, this kind of approach requires a lot of efforts and iterations, and also it requires to have the final product, or at least a representative mock-up available for test.

To EASA opinion, this is the only appropriate way to address the generic aspects of human error in the context described above.

EASA consider that even if human error could be quantified, it would always be negatively impacted by large variance, therefore, it shall never be used for mitigation of risks.

2.2. Non-coherent definition of SW development assurance levels

The proposed OSA does not seem to apply DAL assignment processes in line with guideline of ED-79A section 5.2. For instance, p.46 of the document, one can read:
"Future Datalink implementations within aircraft systems are expected to be at least ED12B/DO178B based Design Assurance Level C (DAL C) and within ground systems at least ED109/DO278 based Assurance Level 4 (AL4) or the equivalent EUROCONTROL/ SWAL3, respectively."

According to ED109A section 2.3.3, an equivalent level of ED12B/DO178B based Design Assurance Level C (DAL C) is ED109/DO278 based Assurance Level 3 (AL3) and not AL4.

Additionally, ED12B/DO178B standard is now superseded by ED12C/DO178C. It is thus suggested not to reference the version of the standard and to state that the latest standard needs to be considered by the industry.

EASA recommends to the Working group to keep the equivalent levels as indicated in the EUROCAE RTCA standards (ED-109A Table 2.2 CNS/ATM TO AIRBORNE LEVEL ASSOCIATION)

TABLE 2-2: CNS/ATM TO AIRBORNE LEVEL ASSOCIATION

ED-109A Assurance Level	ED-12C Software Level
AL1	A
AL2	B
AL3	C
AL4	No Equivalent
AL5	D
AL6	E

2.3. Issues within the assessment

2.3.1. Issue with regards to independence

The OSA does not address the necessary checks of independence claims being used in the assessment (for instance the independence between functions, systems or items that were used while elaborating the different fault trees embedded in section B.6).
This is a fundamental point which needs to be addressed by EUROCAE WG-78 since the conclusion of the OSA in terms of safety requirements could be invalidated.

In this perspective, EASA recommends:

- the use of the ARP4761 and ARP4754A/ED-79A standards which provides guidelines on Common Cause Analysis,
- a check of the validity of this OSA's conclusion.

More generally, the safety assessment approach used to generate this OSA is questioned. Indeed, the safety assessment performed was not driven by a functional or system approach.
On the contrary, the used approach was based on the identification of the failure modes of a given application (in this case the CPDLC application), i.e. a FMEA.
The problem linked to the proposed approach is that the interactions of the different systems supporting a given function are missed. In particular, the potential common modes impacting a specific function are not analysed.

For these reasons, in case SC-214/WG-78 is willing to use the result of this OSA to define appropriate minimum safety requirements for the CPDLC application, EASA recommends to revise this OSA using current aircraft development safety assessment techniques which have proved to be systematic and reliable, e.g.

- Functional Hazard Assessment (FHA) which will allow identifying and classifying the failure condition(s) associated with the functions as listed in paragraph B.1
- Preliminary Safety Analysis (PSSA) which will allow determining the safety related design requirements to be allocated to each domain (ATSU, ACSP, Airborne).

It is to be noted that such FHA/PSSA approach is consistent with the EUROCONTROL SAM[1] (safety assessment methodology) process.
EASA also highlights that it is not addressed when independence between hazards and Environmental conditions or "External Mitigation Means" cannot be demonstrated. For example, EASA considers that the OSA should address independence between the ATSU HMI regarding surveillance indications and the HMI to manage CPDLC. To allow that implementations keep under the same HMI means both surveillance means and CPDLC means, the OSA should assess it and provide the adequate requirements.

2.3.2. Common modes

Regarding common modes of failure, EASA considers that the separation between "single aircraft" and "multiple aircraft" is not adequate. Indeed, there are only two Hazards "loss of CPDLC" and "reception of erroneous/misleading message", but the effects are different depending at which domain the failure occurs. When the failure occurs at aircraft level, it affects only to this aircraft, but when the failure occurs at ATSU or CSP level, it may affect several aircraft.

[1] Cf. http://www.eurocontrol.int/safety/public/site_preferences/display_library_list_public.html#17 , SAM V2.1 electronic

EASA recommends the SC-214/WG-78 to review Table B-1, Table B-6 to B-12, and reassess the effects separately when one aircraft is involved or when several aircraft are involved due to ATSU or CSP failures.

2.3.3. Worst cases and identification of the precise intended use of the functions supported by CPDLC.

EASA considers that there is a lack of systematic assessment, which leads to a lack of identification of risks linked with the intended use and with the type of operations.

- Concerning the use of CPDLC in taxi, EASA identifies that it is not assessed any risk of "undetected misleading/erroneous clearance" intended to cross runways in low visibility conditions. Indeed, for clearances in taxi phase, the increase of crew workload in case of any undetected misleading/erroneous clearance/data has not been validated to provide the same risk figures as for cruise phase.
- Concerning the use of CPDLC in terminal area, the worst case is not identified which could be: "undetected misleading/erroneous clearance" when approaching to runway in parallel runway configuration, or in congested Terminal Area (there are always aircraft in the vicinity). Moreover, the risk due to the future lack of awareness between VFR and IFR flights is not assessed. It is not estimated that new risks will come due to the fact that most of the airports will manage IFR aircraft through CPDLC and VFR aircraft by radio.

EASA considers that OSA should analyse the worst cases of the scenarios where these CPDLC new services are intended to be used, in order to identify the safety requirements to mitigate such cases. Indeed, a complete analysis would identify type of operations which should be forbidden due to the fact that safety hazards could not be properly mitigated for certain environments, or by the proposed technology.

2.3.4. HW failures

The document does not address HW failures and assignment of HW DALs although it is done for SW. EASA considers this is a fundamental point which needs to be addressed by SC-214/WG-78.

However, EASA considers that SW and HW should be addressed as recommendations (not as requirements), because SW and HW requirements are very dependent on the system and equipment design, which in turn is linked to the solution proposed at each domain level. EASA recommends SC-214/WG-78 to identify safety requirements for the functions, which should be converted in DAL requirements at each domain level for the pieces of SW and HW involved in such functions.

2.3.5. No safety objective for DLIC service

The statement "there is no hazard or safety objective associated with the DLIC service" is not understood.

The initialization function of the CPDLC should be part of the OSA analysis; in particular the effect of the loss of this CPDLC initialization function or its erroneous malfunction should be assessed.
It is expected that the loss of the initialization function is at least minor since it should have an impact at minimum equivalent to the Operation Hazard OH-CPDLC-1: "Loss of CPDLC capability [single aircraft]".

EASA highlights that in these days, due to the fact of the existence of two different Data Link technologies (ATN B1 and FANS 1/A+), certain installations require that flight crew do a manual log-off and a manual log-on to transfer from one to the other Data Link technology. This means that DLIC failures may have an effect in flight.

EASA highlights that a systematic safety assessment requires to analyse all the potential failures (even if they seem to have an effect lower than the worst case).

EASA recommends to analyse this hazard taking into account realistic scenario, which can be foreseen during the coexistence of more than one Data Link protocol.

2.3.6. Issue with regards to classification of hazards

A. The proposed classification for the case when the Operation Hazard OH-CPDLC-1 is detected (SC5) is not in line with the Severity Class proposed in ED-78A section.
Indeed, according to this standard, a "Slight increase in workload" on the "Aircraft Crew" should be classified SC4 (and not SC5).

Same comment applies to the Operation Hazard OH-CPDLC-3: Reception of a corrupted CPDLC message [single aircraft] (see section B3.4.3 page 9).

B. The OSA considers in the same way "ENR-1", "TMA" and "APT". EASA considers that these 3 phases are different and should be analysed separately. The cockpit workload is totally different during these phases, therefore the safety assessment should be separated in order to provide adequate results. For example, at table B-4, EASA considers that undetected loss of CPDLC capability for a single aircraft should be considered as SC4 in ENR-1 (as it involves slight increase of crew workload), while such failure should be re-assessed in TMA or APT, as it may include significant increase of workload for flight crew, which should lead to SC3.

C. At Table B-6 the OSA mentions that undetected misleading message (corrupted) has identical severity in any phase. EASA believes that the acceptance and execution of an erroneous clearance in TMA or in Taxi has higher severity that in cruise phase. Indeed, due to the potential lack of independence between hazard and the "EMM" (surveillance), the worst case to be identified is congested TMA or congested airport where there will be always aircraft in the vicinity and Severity to consider should be SC2 (when independence with EMM cannot be demonstrated) and SC3 (when independence can be demonstrated).

D. EASA recommends SC-214/WG-78 to review and reassess table B-6. One of the cases identified, "undetected reception of a misleading/erroneous/corrupted ACM message" (Voice transfer message) leads to an undetected complete loss of communications between Pilot and Controller (loss of CPDLC + loss of voice communications). EASA recommends SC-214/WG-78 to discuss the severity associated to this case for the worst scenario foreseen (TMA during approach and landing).

E. Loss of CPDLC Undetected. EASA considers that in any case, at least there is an increase of workload at flight crew level, therefore the SC to consider should be SC4. Additionally, EASA recommends SC-214/WG-78 to discuss the effect of this hazard when aircraft is in TMA of in APT, as the undetected loss of CPDLC may lead to higher severity, especially when it involves several aircraft. EASA recommends SC-214/WG-78 to assess the expected increase of workload for the controller in case of undetected loss of CPDLC affecting to several aircraft.

The severity classification of the OHs presented in Table B-17 needs to be revised considering these comments.

2.3.7. Unit conversion

The conclusion of this OSA relies on a certain number of assumptions (e.g. number of CPDLC messages per flight and per FH for an aircraft, driven by the duration of the flight, …) which do not seem to have been validated and which could possibly not take into account the worst case.

EASA considers that certain number of messages do not depend on the duration of the flight (as for the APR and TMA phases), therefore the conversion is not done properly. EASA considers that the number of messages foreseen in TMA or APT will not be duplicated because the flight time is 4 hours, or reduced for a 1 hour flight. EASA recommends SC-214/WG-78 to review Table B-14.

EASA's concern is that the derived safety requirements on the CPDLC application could possibly not be stringent enough.

2.3.8. Questionable assumptions

A.
The validity of the assumption:

> "*ASSUMP-CPDLC-3 It is assumed that the probability of success of EMM-CPDLC-1 is 0.99*
> *Note: It has been conservatively considered that 99/100 unexpected manoeuvres will be detected by the controller (through available surveillance means: EC-CPDLC-3) in time to implement corrective instructions.*"

is not demonstrated and questionable. Indeed, according to AMC 25.1309 §12:

- *quantitative assessments of crew errors are not considered feasible*
- *reasonable tasks are those for which full credit can be taken because they can realistically be anticipated to be performed correctly when they are required or scheduled*
- *unless flight crew actions are accepted as normal airmanship, they should be described in the approved Aeroplane Flight Manual.*

EASA suggests to have the same approach in this safety assessment, i.e. the EMM should correspond to reasonable tasks only either accepted as normal controllership or described in an approved procedure, recognized worldwide (in order to be able to take credit of it in the scope of the elaboration of the CPDLC standard).

Moreover, the assumption ASSUMP-CPDLC-3 does not take into account the reliability of the surveillance mean to provide the controller with information to enable him/her to take appropriate corrective action.

B.
The validity of the assumption:
"ASSUMP-CPDLC-4. It is assumed that the probability of having one aircraft in the vicinity is 24.10-3"
is not demonstrated and thus questionable. Indeed this assumption does not seem to be derived from international recognized values and does not seem to take into account the future growth in traffic by a factor of 3 (refer to D2.4.3-01 - White Paper on the SESAR Safety Target, available at this address: http://www.episode3.aero/public-documents). Additionally, this assumption is questioned specially for the phases of Taxi, Take-off and Approach and landing, where such probability is not adequate as it is used as a mitigating factor.

2.3.9. Removal of human error contribution from all fault tree analyses

The following comments are related to the following basic causes:

- CT-CPDLC-1 "Controller does not detect the incorrect DM"
- FC-CPDLC-2 "FC does not detect the incorrect DM"

As already mentioned in previous comment, the basic causes "Controller does not detect the incorrect DM" and "FC does not detect the incorrect UM" are questionable. Indeed according to AMC 25.1309 §12:

- *quantitative assessments of crew errors are not considered feasible*
- *reasonable tasks are those for which full credit can be taken because they can realistically be anticipated to be performed correctly when they are required or scheduled*
- *unless flight crew actions are accepted as normal airmanship, they should be described in the approved Aeroplane Flight Manual.*

EASA recommends SC-214/WG-78 to remove the human errors contribution from the different fault trees used in this OSA.

EASA proposed approach to solve this concern will allow as well to fix other inconsistencies found in the document; for instance between:

- Figure B-3 where a probability of 6.4e-2 is taken as an assumption for the basic cause CT-CPDLC-1 "Controller does not detect the incorrect DM", and
- Table B-23 where no safety requirements is derived for this basic cause.

2.3.10. Issue with regards to the terminology used in the OSA

The so-called "safety requirements" listed in Table B-21 are:

- in the frame of airborne systems certification not called safety requirements but functional requirements,
- are not traceable to any assessment performed previously within the document.

For this reason, EASA highly recommends to:

- make the distinction between functional/performance requirements and safety requirements in order to stay in line with already available industry standards,
- build the fault trees taking into account the functional/performance requirements to derive the safety requirements (and not give the impression of the contrary).

2.3.11. Additional comments

2.3.11.a

The following comment is related to the following basic cause:

FC-CPDLC-1 "FC enters incorrect information for DM"

Considering the derived "safety" requirements related to this basic cause quoted in Table B-23:

- SR-AC-CPDLC-14: The aircraft system shall prevent release of a report/operational response without flight crew action.
- SR-FC-CPDLC-01: The flight crew shall check the correctness and the appropriateness of every message before sending it.
- SR-FC-CPDLC-03: The flight crew shall respond to a message in its entirety

a human error of the FC when entering the information will be detected by the FC during the confirmation phase requested by requirement SR-AC-CPDLC-14, SR-FC-CPDLC-01, SR-FC-CPDLC-03.

This means that:

- Only the AC system can corrupt the message without possibility of detection

EASA recommends SC-214/WG-78 to remove basic cause FC-CPDLC-1 "FC enters incorrect information for DM" from the fault tree.
EASA also recommends to review Table B-1 (page 4) as OH-CPDLC-3 description indicates that corruption is introduced by the human.

2.3.11.b

The following comment is related to the following basic causes:

- *AC-CPDLC-1 "AC system corrupts the DM"*
- *AC-CPDLC-2 "AC system fails to detect corruption of DM"*

EASA understanding is that only the AC system can corrupt the message, not the pilot. If this understanding is correct, this means that the 2 basic causes AC-CPDLC-1 and AC-CPDLC-2 are in fact the same.

EASA suggestion is to group those 2 basic causes in only one, e.g.: "Undetected corruption of the DM by the AC system".

Same comment applies to the basic causes:

- *GD-CPDLC-1 "GND system corrupts the DM"*
- *GND-CPDLC-2 "AC system fails to detect corruption of DM"*

2.3.11.c

What is the rationale justifying the fact that ACSP can corrupt a message without any safety effect? Some fault trees show that probability of ACSP to corrupt a message is =1.
In order to state that any corruption done at ACSP level has not any safety effect, it requires the introduction of safety requirements, as the need of checksums or CRC within the messages, and requirements to the end systems to detect any corruption when breach of the checksums. This requirements have to be analysed, as also require certain level of assurance development linked to the risk of failure of such detection mechanisms.

2.3.11.d

Purpose and scope. The list of "functions" being supported by the CPDLC application and enumerated at the beginning of section B.1 does not seem to be in line with the list of "services" enumerated in the second half of the same section.

3. Conclusion

EASA considers that the results of this OSA are not complete in order to consider this standard as the MoC to certify the safety of either ground or airborne installation for these new proposed kinds of operation.

Moreover the terminology and methodology used to produce this OSA do not seem to be:

- consistent with the current airborne systems regulatory framework (refer to CS-25.1309 and associated AMC), and
- compatible with the already available industry standards (in particular EUROCAE ED-79A and SAE ARP4761).

Besides, EASA does not agree with the severity classes and safety objectives proposed in table B-18. Due to this, EASA cannot agree with the results of the proposed OSA.

Recommendation:

EASA recommends to re-assess the OSA taking into consideration the comments provided, and also defining with more rigour the intended purpose of the existing and the new functionalities. This will allow to identify the appropriate operational limitations, where the risks cannot be adequately mitigated by technology. Additionally, it will provide the adequate guidance to be observed as MoC.